Identity Theft Handout

Please note that this Information Paper only provides basic information and is not intended to serve as a substitute for personal consultations with a Legal Assistance Attorney.

INTRODUCTION

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game; rent a car, mail your tax returns, change service providers for your cell phone, or apply for a credit card. In each transaction, you reveal bits of personal information, like your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address, and phone numbers – a goldmine of information for an identity thief. Once a thief has that information, it can be used without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend time and money cleaning up the mess the thieves have made of their good name and credit record. They may lose out on job opportunities, and loans for education, housing, or cars. They may even get arrested for crimes they didn't commit.

Can you prevent an identity theft? As with any crime, you cannot completely control whether you will become a victim. But according to the Federal Trade Commission (FTC), the nation's consumer protection agency, you can minimize your risk by managing your personal information cautiously.

HOW IDENTITY THEFT OCCURS

Skilled identity thieves use a variety of ways to gain access to your personal information. For example, they may get information from businesses or other institutions by stealing it while they're on the job; bribing an employee who has access to these records; hacking these records; and conning information out of employees. Or:

- they may steal your wallet or purse.
- they may steal your personal information through email or the phone by saying they're from a legitimate company and claiming that you have a problem with your account. This practice is known as "phishing" online or "pretexting by phone.
- they may steal your credit or debit card numbers by capturing the information in a data storage device in a practice known as "skimming." They may swipe your card for an actual purchase, or attach a device to an ATM machine where they may enter or swipe your card.
- they may get your credit reports by abusing the authorized access that was granted to their employer, or by posing as a landlord, employer, or someone else who may have a legal right to your report.
- they may rummage through your trash, the trash of businesses, or public trash dumps in a practice known as "dumpster diving."

- they may steal personal information they find in your home.
- they may steal your mail, including bank and credit card statements, credit card offers, new checks, and tax information.
- they may complete a "change of address form" to divert your mail to another location.

Once identity thieves have your personal information, they may use it to commit fraud or theft. For example:

- they may call your credit card issuer to change the billing address on your account. The imposter then runs up charges on your account. Because the bills are being sent to a different address, it may be some time before you realize there's a problem.
- they may open new credit card accounts in your name. When they use the credit cards and don't pay the bills, the delinquent accounts are reported on your credit report.
- they may establish phone or wireless service in your name.
- they may open a bank account in your name and write bad checks on the account.
- they may counterfeit checks or credit or debit cards, or authorize electronic transfers in your name, and drain your bank account.
- they may file for bankruptcy under your name to avoid paying debts they've incurred under your name, or to avoid eviction.
- they may buy a car by taking out an auto loan in your name.
- they may get identification such as a driver's license issued with their picture, in your name.
- they may get a job or file fraudulent tax returns in your name.
- they may give your name to the police during an arrest. If they don't show up for the court date, a warrant for arrest is issued in your name.

IF YOUR PERSONAL INFORMATION HAS BEEN LOST OR STOLEN

If you've lost personal information or identification, or if it has been stolen from you, you can minimize the potential for identity theft if you act quickly.

- **Financial accounts:** Close accounts, like credit card and bank accounts, immediately. When you open new accounts, place passwords on them. Avoid using your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

- **Social Security number:** Call the toll-free fraud number of any of the three nationwide consumer reporting companies and place an initial fraud alert on your credit reports (see page19). An alert can help stop someone from opening new credit accounts in your name.

- **Driver's license/other government-issued identification:** Contact the agency that issued the license or other identification document. Follow its procedures to cancel the document and to get a replacement. Ask the agency to flag your file so that no one else can get a license or any other identification document from them in your name.

Once you have taken these precautions, watch for signs that your information is being misused, and that your identity has been stolen.

If your information has been misused, file a report about the theft with the police, and file a complaint with the FTC, as well. If another crime was committed – for example, if your purse or wallet was stolen or your house or car was broken into – report it to the police immediately.

HOW CAN YOU TELL IF YOU'RE A VICTIM OF IDENTITY THEFT?

If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from the three nationwide consumer reporting companies. If you have lost any personal information – or if it has been stolen – you may want to check all your reports more frequently for the first year. Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

- failing to receive bills or other mail. This could mean an identity thief has submitted a change of address.
- receiving credit cards for which you did not apply.
- denial of credit for no apparent reason.
- receiving calls from debt collectors or companies about merchandise or services you didn't buy.

IDENTITY THEFT VICTIMS: IMMEDIATE STEPS

If you are a victim of identity theft, take the following four steps as soon as possible, and keep records of your conversations and copies of all correspondence. You also should get a copy of the FTC publication, *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide that describes what to do, your legal rights, how to handle specific problems you may encounter on the way to clearing your name, and what to watch for in the future. The guide also includes the ID Theft Affidavit to help you report information to many companies. For more information, see www.consumer.gov/idtheft.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You need to contact only one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order free copies of your credit reports, and, if you ask, only the last four digits of your SSN will appear on your credit reports. Once you get your credit reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information like your SSN, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, contact the consumer reporting companies to get it removed. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

FRAUD ALERTS

- **An initial alert stays on your credit report for at least 90 days.** You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or could be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. When you place an initial fraud alert on your credit report, you're entitled to one free credit report from each of the three nationwide consumer reporting companies.

- **An extended alert stays on your credit report for seven years.** You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an "identity theft report" (see page 20). When you place an extended alert on your credit report, you're entitled to two free credit reports within 12 months from each of the three nationwide consumer reporting companies.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your SSN, name, address, and other personal information requested by the consumer reporting company.

When a business sees the alert on your credit report, they must verify your identity before issuing you credit. As part of this verification process, the business may try to contact you directly. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak to someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. *It's important to notify credit card companies and banks in writing.* Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or on fraudulently opened accounts, ask the company for the forms to dispute those transactions.

For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, write a letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit. If not, ask the representative to send you the company's fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information.

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your

best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

IDENTITY THEFT REPORTS

An identity theft report may have two parts:

Part One is a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your state Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. When you file a report, provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened, and the alleged identity thief.

Part Two of an identity theft report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the consumer reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your identity theft report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your identity theft report as incomplete. You will have to resubmit your identity theft report with the correct information.

3. **File a report with your local police or the police in the community where the identity theft took place.**

Then, get a copy of the police report, or at the very least, the number of the report. It can help you deal with creditors who need proof of the crime. If the police are reluctant to take your report, ask to file a "Miscellaneous Incidents" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

4. **File a complaint with the Federal Trade Commission.**

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

You can file a complaint online at www.consumer.gov/idtheft. If you don't have Internet access, call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TDD: 202-326-2502; or write: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Be sure to call the Hotline to update your complaint if you have any additional information or problems.

Also be sure to utilize the FTC's Military Sentinel Program. Military Sentinel is a project of the Federal Trade Commission and the Department of Defense to identify and target consumer protection issues that affect members of the United States Armed Forces and their families. Military Sentinel allows members of the United States Armed Forces to enter consumer complaints directly into a database that is immediately accessible by over 500 law enforcement organizations throughout the United States, Canada, and Australia. These law enforcement agencies use this complaint data to target cases for prosecution and other enforcement measures.

ACTIVE DUTY FRAUD ALERTS

If you are a member of the military and away from your usual duty station, you may place an active duty alert on your credit reports by contacting any one of the three major consumer reporting companies listed on page 2. Active duty alerts can help minimize the risk of identity theft while you are deployed. To place an alert on your credit report, or to have it removed, you will have to provide appropriate proof of your identity, including your SSN, name, address, and other personal information requested by the consumer reporting company. You may use a personal representative to place or remove an alert.

Active duty alerts are in effect on your report for one year. If your deployment lasts longer, you can place another alert on your credit report.

When a business sees the alert on your credit report, they must verify your identity before issuing any credit. As part of this verification process, the business may try to contact you directly. Be sure to keep your contact information updated, or you may experience delays if you are applying for new credit.

When you place an active duty alert on your credit report, you'll also be removed from the credit reporting companies' marketing list for prescreened credit card offers for two years unless you ask to be put back on the list before then.

FOR MORE INFORMATION

The FTC publishes a series of publications about the importance of personal information privacy. To request free copies of brochures, visit ftc.gov or call 1-877-FTC-HELP (382-4357).

For further information or help feel free to make an appointment with a Legal Assistance Attorney, DSN 421-4152, Civ 0711-729-4152.

REVIEWED BY: CPT Michael Watts, Chief, Client Services
DATE: 18 July 2006

References:

Federal Trade Commission Website - http://www.consumer.gov/idtheft/

Federal Trade Commission Website Military Sentinel Program - http://www.consumer.gov/military/index.htm

FTC ID Theft Guidebook - http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

JAG Website - http://www.jagcnet.army.mil/legal (click on Money Matter, then Personal Financial Privacy Information, then scroll down until you see ID Theft)